CHAPTER 3

Configuring ISDN

This chapter describes how to configure a Cisco 1600 series router to dial into a central-site router over an Integrated Services Digital Network (ISDN) line and provides verification steps and troubleshooting tips.

This chapter contains the following sections:

- Before You Begin
- Internet Protocol
- Internet Packet Exchange Protocol
- ISDN Leased Line
- How ISDN Works

Before You Begin

The configurations in this chapter are based on the following assumptions:

- Your Cisco 1600 hardware is correctly installed according to the *Cisco 1600 Series Hardware Installation Guide* that came with the router.
- Your Cisco 1600 is dialing into a central-site router.
- Your Cisco 1600 is using multilink Point-to-Point Protocol (PPP).
- Your ISDN line is installed and correctly configured. See the "Configuring the ISDN Line" chapter in the *Cisco 1600 Series Hardware Installation Guide* for more information on ordering and configuring your ISDN line.

Before you begin configuration, be aware of the following:

- You need to enter the commands in the order shown in the task tables.
- The values shown in italics are examples. You should substitute the values shown with values that are appropriate for your network.
- You should be familiar with Cisco IOS software and its conventions.

Note In order to use the verification steps described in this chapter, you must be familiar with Cisco IOS commands and command modes. When you use the verification steps, you need to change to different command modes. If you are not familiar with command modes, refer to the "Understanding Command Modes" section in the "Configuring ISDN" chapter.

Internet Protocol

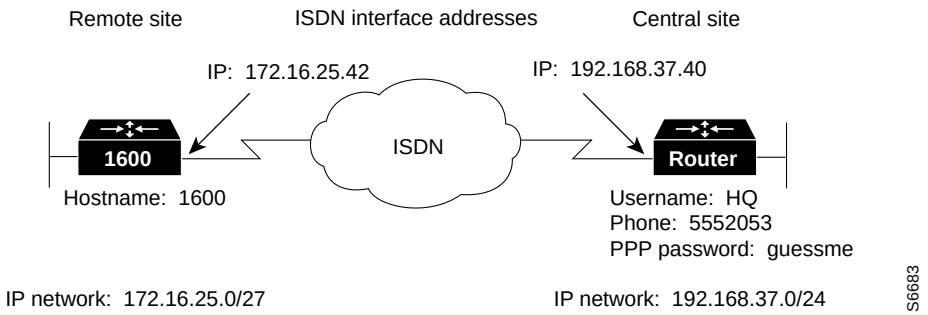
This section describes how to configure your Cisco 1600 for Internet Protocol (IP) when dialing out over an ISDN line. You should configure your router for IP if you want to use Internet services, such as the World Wide Web, or if the network that you are dialing into uses IP.

These are the major tasks when configuring your router:

- Configuring Global Parameters
- Configuring Security
- Configuring the Ethernet Interface
- Configuring the ISDN Interface
- Configuring Static Routes and Dialing Behavior
- Configuring Command Line Access to the Router

Figure 3-1 illustrates the example configuration used in this section.

Figure 3-1 ISDN Example Configuration—IP



Configuring Global Parameters

Use this table to configure the router for some global parameters, including the ISDN switch type that the router is connected to through the ISDN line, and how log and debug messages are timestamped.

		Prompt	Command
Step 1	Enter configuration mode.	Router#	configure terminal
Step 2	Configure the router to show the date and time of all debug messages. This command is optional, but recommended if you use debug commands to troubleshoot your configuration.	Router(config)#	service timestamps debug datetime msec
Step 3	Configure the router to show the date and time of all log messages. This command is optional, but recommended if you use the verification steps described in this guide. This feature is enabled for all the example command output shown in this guide.	Router(config)#	**service timestamps log** *datetime msec*

		Prompt	Command
Step 4	Configure the type of central office switch used on the ISDN interface. Use the keyword that matches the ISDN switch type that you are using: basic-ts013 —Australian TS013 switches basic-1tr6 —German 1TR6 ISDN switches basic-nwnet3—Norway NET3 switches (phase 1) basic-net3—NET3 ISDN switches vn2—French VN2 ISDN switches vn3—French VN3 ISDN switches ntt—Japanese NTT ISDN switches basic-5ess—AT&T basic rate switches basic-dms100—NT DMS-100 basic rate switches basic-ni1—National ISDN-1 switches basic-nznet3—New Zealand Net3 switches	Router(config)#	**isdn switch-type** *basic-ni1*

Configuring Security

Use this table to configure the router with some security measures, including the password used to access the router and the username and password used for Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) authentication with the central-site router.

		Prompt	Command
Step 1	Specify a password to prevent unauthorized access to the router.	Router(config)#	**enable password** *1600user*

		Prompt	Command
Step 2	Configure the router with a host name, which is used in prompts and default configuration file names. For PPP authentication, the host name entered with this command must match the username of the central-site router.	Router(config)#	**hostname** *1600*
Step 3	Specify the password used during caller identification and CHAP and PAP authentication. For CHAP and PAP authentication, the username entered with this command must match the host name of the central-site router.	1600(config)#	**username *HQ* password *guessme***

Configuring the Ethernet Interface

Use this table to configure the Ethernet interface (which connects the router to your local network) with an IP address. This gives your router a unique address on your local network.

		Prompt	Command
Step 1	Enter configuration mode for the Ethernet interface.	1600(config)#	**interface Ethernet0**
Step 2	Configure this interface with an IP address and a subnet mask.	1600(config-if)#	**ip address** *172.16.25.42 255.255.255.224*
Step 3	Enable the interface and the configuration changes you have just made on the interface.	1600(config-if)#	no shutdown
Step 4	Exit configuration mode for this interface.	1600(config-if)#	**exit**

Verifying Your Configuration

You can verify your configuration by checking that the Ethernet interface has the correct IP address:

Step 1 From the privileged EXEC command mode, enter the **show arp** command:

```
1600# show arp
```

Step 2 You should see command output similar to the following:

```
Protocol Address          Age (min)   Hardware
Addr    Type   Interface
Internet 171.16.25.42           -     0060.834f.66dd    ARPA   Etherne
t0
1600#
```

Step 3 The IP address (shown in bold in the example) should be your router Ethernet IP address and should match the IP address that you entered with the **ip address** command.

Step 4 To continue configuration, re-enter global configuration mode.

Configuring the ISDN Interface

Use this table to configure the ISDN interface (which connects the router to the WAN) for the following:

- Dial-on-Demand Routing (DDR) so that the router automatically dials the remote site when it receives a certain amount of data traffic.
- PPP packet encapsulation so that the router can use specific PPP functions.
- PPP authentication so that the router is authenticated by the central-site router using one of two standard PPP authentication methods—Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP).
- Multilink PPP so that the router can send data to the same destination over multiple point-to-point data links.

		Prompt	Command
Step 1	Enter configuration mode for the ISDN interface.	1600(config)#	**interface BRI0**
Step 2	Add a description of this interface to help you remember what is attached to the interface.	1600(config-if)#	**description** *ISDN connectivity*
Step 3	Define the service profile identifier (SPID) number assigned by the ISDN service provider to the B1 channel. This step is required only when the service provider has assigned a SPID to your ISDN line. Not all ISDN lines have SPIDs.	1600(config)#	**isdn spid1** *555987601*
Step 4	Define the SPID number assigned by the ISDN service provider to the B2 channel. This step is required only when the service provider has assigned a SPID to your ISDN line. Not all ISDN lines have SPIDs.	1600(config)#	**isdn spid2** *555987602*
Step 5	Enable IP routing on this interface without assigning an IP address.	1600(config-if)#	**ip unnumbered Ethernet0**
Step 6	Configure this interface to place a call to multiple sites and to authenticate calls from multiple sites based on IP address and dialer string (phone number). The name you enter after the **name** keyword in this command must match the name entered with the **username** command in the previous "Configuring Security" section.	1600(config-if)#	**dialer map ip** *192.168.37.40* **name** *HQ 5552053*
Step 7	Configure bandwidth on demand by setting the maximum load before the router places another call to a destination.	1600(config-if)#	**dialer load-threshold** *70*
Step 8	Assign the dialer interface to a dialer group.	1600(config-if)#	**dialer-group** *1*
Step 9	Set the encapsulation method on this interface to PPP.	1600(config-if)#	**encapsulation ppp**

		Prompt	Command
Step 10	Enable CHAP and PAP authentication on this interface. CHAP authentication is attempted first. If the central-site router does not support CHAP, PAP is used for authentication.	1600(config-if)#	**ppp authentication chap pap callin**
Step 11	Enable multilink PPP on this interface.	1600(config-if)#	**ppp multilink**
Step 12	Enable the interface and the configuration changes you have just made on the interface.	1600(config-if)#	no shutdown
Step 13	Exit configuration mode for this interface.	1600(config-if)#	**exit**

Verifying Your Configuration

You can verify your configuration to this point by confirming the ISDN line status:

Step 1 From the privileged EXEC command mode, enter the **show isdn status** command.

Step 2 You should see command output similar to the following:

```
1600# show isdn status
The current ISDN Switchtype = basic-5ess
ISDN BRI0 interface
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 80, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        No Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 0
    Total Allocated ISDN CCBs =
```

Step 3 Confirm that the current ISDN switch type (shown in bold in the example) matches the actual switch type that you are using.

Step 4 Confirm that the “Layer 1 status: ACTIVE” message (shown in bold in the example) appears in the command output.

Step 5 Confirm that the “State = MULTIPLE_FRAME_ESTABLISHED” message (shown in bold in the example) appears in the command output.

Note In some cases, you might see a "State = TEI_ASSIGNED" message instead of the "State = MULTIPLE_FRAME_ESTABLISHED" message. This message also means that the ISDN line is correctly configured.

Step 6 To continue configuration, re-enter global configuration mode.

Tips

If you are still having problems, do the following:

- Make sure that you entered the **no shutdown** command for the ISDN interface while in interface configuration mode. This enables the configuration changes that you made on the interface.
- Make sure that any external NT-1 is functioning correctly. Refer to the documentation that came with the NT-1.
- Make sure the ISDN line is correctly configured by checking with the ISDN service provider.

Configuring Static Routes and Dialing Behavior

Use this table to configure some parameters that control how and when the router dials the central-site router, including:

- Static IP routes to the central-site router, which tell your router where to send data.
- Access lists, so that specific types of data trigger a call to the remote site and control the amount of time that your router remains connected to the remote site when no specific type of data is being sent.
- A dialer list, which controls the how and when the router dials the remote site, based on the access lists.

		Prompt	Command
Step 1	Establish a static IP route to the remote network.	1600(config)#	**ip route** *0.0.0.0 0.0.0.0 192.168.37.40*
Step 2	Establish a static IP route to the central-site router through this interface.	1600(config)#	**ip route** *192.168.37.40 255.255.255.255* **BRI0**
Step 3	Define a standard access list based on Internet Control Message Protocol (ICMP) traffic.	1600(config)#	**access-list** *101 permit icmp any any*
Step 4	Define a standard access list based on IP traffic.	1600(config)#	**access-lis**t *101 permit ip any any*
Step 5	Specify an dialer list by list number and protocol (IP) to define the "interesting" packets that can trigger a call to the destination.	1600(config)#	**dialer-list** *1* **protocol ip list** *101*

Verifying Your Configuration

You can verify your configuration to this point by:

- Confirming the Static IP Route.
- Confirming Connectivity to the Central-Site Router.
- Confirming Multilink PPP Configuration for the B1 Channel.
- Confirming Multilink PPP Configuration for the B1 Channel.
- Confirming Multilink PPP Configuration for the B2 Channel.

Confirming the Static IP Route

You can verify your configuration by confirming the static IP route:

Step 1 From the privileged EXEC command mode, enter the **show ip route** command.

Substitute the IP address of the central-site router ISDN interface for the IP address shown in the example.

Step 2 Confirm that the “directly connected via BRI” message (shown in bold in the example) appears in the command output:

```
1600# show ip route 192.168.37.40
Routing entry for 192.168.37.40/32
  Known via "connected", distance 0, metric 0 (connected)
  Routing Descriptor Blocks:
 * directly connected, via BRI0
      Route metric is 0, traffic share count is 1
```

Step 3 To continue configuration, re-enter global configuration mode.

Confirming Connectivity to the Central-Site Router

You can verify your configuration by confirming connectivity to the central-site router:

Step 1 From the privileged EXEC command mode, enter the **ping** command followed by the IP address of the central-site router:

```
1600# ping 192.168.37.40
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.37.40, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 40/43/48 ms
1600#
*Mar  1 03:37:46.526: %LINK-3-UPDOWN: Interface BRI0:1, changed state
to up
*Mar  1 03:37:46.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
BRI0:1, changed state to up
*Mar  1 03:37:46.939: %LINK-3-UPDOWN: Interface Virtual-Access1,
changed state to up
*Mar  1 03:37:47.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to up
 *Mar  1 03:35:57.217: %ISDN-6-CONNECT: Interface BRI0:1 is now
connected to 5552053 HQ
```

Step 2 Note the percentage in the “Success rate...” line (shown in bold in the example). If the success rate is 60 percent (3/5) or greater, your router is successfully transferring data to the central-site router.

Step 3 To continue configuration, re-enter global configuration mode.

Confirming Multilink PPP Configuration for the B1 Channel

This verification step is supported in Cisco IOS software release 11.2 and later.

Step 1 From the privileged EXEC mode, confirm that the ISDN is connected to the remote site by entering the **ping** command followed by the IP address of the central-site router:

```
1600# ping 192.168.37.40
```

Step 2 Enter the **show ppp multilink** command.

Step 3 Confirm that the "Master link is Virtual-Access1" message (shown in bold in the example) appears in the command output.

```
1600# show ppp multilink
 Bundle HQ, 1 member, Master link is Virtual-Access1
Dialer Interface is BRI0
  0 lost fragments, 0 reordered, 0 unassigned, sequence 0x0/0x0
rcvd/sent
  0 discarded, 0 lost received, 1/255 load
Member Link: 1
BRI0:1
```

Step 4 If you do not see the message in the output, take one or both of the following steps:

- Confirm that multilink PPP is configured on the central-site router that you are connecting to.
- If multilink PPP is configured on the central-site router, use the **show interface** command as described in the following "Confirming Multilink PPP Configuration for the B1 Channel" section.

Step 5 To continue configuration, re-enter global configuration mode.

Confirming Multilink PPP Configuration for the B1 Channel

Step 1 From the privileged EXEC command mode, confirm that the ISDN line is connected to the remote site by entering the **ping** command followed by the IP address of the central-site router:

```
1600# ping 192.168.37.40
```

Step 2 Enter the **show interface virtual-access 1** command.

Step 3 Confirm that the "Open: IPCP" message (shown in bold in the example) appears in the command output:

```
1600# show interface virtual-access 1

Virtual-Access1 is up, line protocol is up
  Hardware is Virtual Access interface
  MTU 1500 bytes, BW 64 Kbit, DLY 100000 usec, rely 255/255, load
1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  DTR is pulsed for 5 seconds on reset
  LCP Open, multilink Open
Open: IPCP
Last input 00:00:01, output never, output hang never
  Last clearing of "show interface" counters 00:54:41
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     708 packets input, 150742 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     709 packets output, 157653 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

Step 4 To continue configuration, re-enter global configuration mode.

Confirming Multilink PPP Configuration for the B2 Channel

Step 1 From the privileged EXEC command mode, confirm that the ISDN line is connected to the remote site by entering the **ping** command followed by the IP address of the central-site router:

```
1600# ping 192.168.37.40
```

Step 2 Create enough network traffic so that the second ISDN B channel dials the remote site.

Step 3 Check the LEDs labeled B1 and B2.

If both LEDs are lit solid, multilink PPP is correctly configured for both ISDN B channels.

If the ISDN line is connected to the router on-board ISDN port, the LEDs are on the front panel of the router. If the ISDN line is connected to a WAN interface card ISDN port, the LEDs are on the front panel of the card.

Step 4 To continue configuration, re-enter global configuration mode.

Tips

If you are still having problems, do the following:

- Confirm that your router is configured with the correct IP address.
- Confirm that you have correctly configure the static IP routes with the **ip route** command.

Configuring Command Line Access to the Router

Use this table to configure some parameters that control access to the router, including the type of terminal line used with the router, how long the router waits for a user entry before it times out, and the password used to start a terminal session with the router.

		Prompt	Command
Step 1	Specify the console terminal line.	`1600(config)#`	**line console** *0*
Step 2	Set the interval that the EXEC command interpreter waits until user input is detected.	`1600(config-line)#`	**exec-timeout** *5*
Step 3	Specify a virtual terminal for remote console access	`1600(config-line)#`	**line vty** *0 4*
Step 4	Specify a password on the line.	`1600(config-line)#`	**password** *lineaccess*
Step 5	Enable password checking at terminal session login.	`1600(config-line)#`	**login**
Step 6	Exit configuration mode.	`1600(config-line)#`	**end**

Troubleshooting IP Problems

If you are having problems or the output that you received during the verification steps is very different from what is shown, you can troubleshoot your router with the Cisco IOS **debug** commands. The **debug** commands provide extensive command output that is not included in this document.

Caution If you are not familiar with Cisco IOS debug commands, you should read the "Using Debug Commands" section in the "Cisco IOS Basic Skills" chapter before attempting any debugging.

Following are **debug** commands that are helpful when troubleshooting ISDN with IP routing. Follow these commands with the **ping** command to begin debug output:

- debug dialer events
- debug isdn q931
- debug ppp negotiation
- debug ppp authentication
- debug ppp multilink events

Internet Packet Exchange Protocol

This section describes a configuration for Internet Packet Exchange (IPX) protocol when dialing out over an ISDN line. You should configure your router for IPX if the network that you are dialing into uses IPX and you want to access the IPX services, such as file servers and printer servers, that are available on that network.

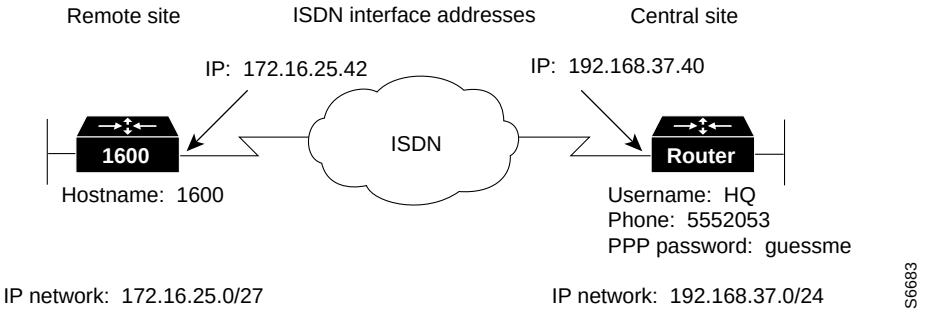
These are the major tasks when configuring your router:

- Configuring Global Parameters
- Configuring Security
- Configuring IPX Routing
- Configuring the Ethernet Interface

- Configuring the ISDN Interface
- Configuring When the Router Dials Out
- Configuring Command Line Access to the Router

Figure 3-2 illustrates the example configuration used in this section.

Figure 3-2 ISDN Example Configuration—IPX



Configuring Global Parameters

Use this table to configure the router for some global parameters, including the ISDN switch type that the router is connected to through the ISDN line, and how log and debug messages are timestamped.

		Prompt	Command
Step 1	Enter configuration mode.	`Router#`	**configure terminal**
Step 2	Configure the router to show the date and time of all debug messages. This command is optional, but recommended if you use debug commands to troubleshoot your configuration.	`Router(config)#`	**service timestamps debug** *datetime msec*

		Prompt	Command
Step 3	Configure the router to show the date and time of all log messages. This command is optional, but recommended if you use the verification steps described in this guide. This feature is enabled for all the example command output shown in this guide.	`Router(config)#`	**`service timestamps log`** `datetime msec`
Step 4	Configure the type of central office switch being used on the ISDN interface. Use the keyword that matches the ISDN switch type that you are using: basic-ts013 —Australian TS013 switches basic-1tr6 —German 1TR6 ISDN switches basic-nwnet3—Norway NET3 switches (phase 1) basic-net3—NET3 ISDN switches vn2—French VN2 ISDN switches vn3—French VN3 ISDN switches ntt—Japanese NTT ISDN switches basic-5ess—AT&T basic rate switches basic-dms100—NT DMS-100 basic rate switches basic-ni1—National ISDN-1 switches basic-nznet3—New Zealand Net3 switches	`Router(config)#`	**`isdn switch-type`** *`basic-ni1`*

Configuring Security

Use this table to configure the router with some security measures, including the password used to access the router and the username and password used for Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) authentication with central-site routers.

		Prompt	Command
Step 1	Specify a password to prevent unauthorized access to the router.	`Router(config)#`	**enable password** *1600user*
Step 2	Configure the router with a host name, which is used in prompts and default configuration file names. For PPP authentication, the host name entered with this command must match the username of the central-site router.	`Router(config)#`	**hostname** *1600*
Step 3	Specify the password used during caller identification and CHAP and PAP authentication. For CHAP and PAP authentication, the username entered with this command must match the host name of the central-site router.	`1600(config)#`	**username** *HQ* **password** *guessme*

Configuring IPX Routing

Use this command to enable IPX routing on the router. The default setting for the router is IPX routing disabled.

`1600(config)#`**ipx routing** *xxxx.xxxx.xxxx*

Configuring the Ethernet Interface

Use this table to configure the Ethernet interface (which connects the router to your local network) with an IPX address. Doing so gives your router a unique address on your local network.

		Prompt	Command
Step 1	Enter configuration mode for the Ethernet interface.	`1600(config)#`	**`interface Ethernet0`**
Step 2	Enable IPX routing on this interface.	`1600(config-if)#`	**`ipx network`** *ABC*
Step 3	Enable the interface and the configuration changes you have just made on the interface.	`1600(config-if)#`	`no shutdown`
Step 4	Exit configuration mode for the interface.	`1600(config-if)#`	**`exit`**

Configuring the ISDN Interface

Use this table to configure the ISDN interface (which connects the router to the WAN) for the following:

- An IPX address, so that the router WAN interface is recognized by the central site IPX network.
- IPX spoofing, so that the router can answer any “watchdog” packets from a server on the local LAN. Then the router does not have to dial the central site location every time it receives a “watchdog” packet destined for the remote network.
- Dial-on-Demand Routing (DDR) parameters, so that the router automatically dials the remote site when it receives a certain amount of data traffic.
- PPP packet encapsulation, so that the router can use specific PPP functions.
- PPP authentication, so that the router is authenticated by the central-site router using one of two standard PPP authentication methods—Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP).
- Multilink PPP, so that the router can send data to the same destination over multiple point-to-point data links.

		Prompt	Command
Step 1	Enter configuration mode for the ISDN interface.	`1600(config)#`	**interface BRI0**
Step 2	Add a description of this interface to help you remember what is attached to the interface.	`1600(config-if)#`	**description** *ISDN connectivity*
Step 3	Define the service profile identifier (SPID) number assigned by the ISDN service provider to the B1 channel. This step is required only when the service provider has assigned a SPID to your ISDN line. Not all ISDN lines have SPIDs.	`1600(config)#`	**isdn spid1** *555987601*
Step 4	Define the SPID number assigned by the ISDN service provider to the B2 channel. This step is required only when the service provider has assigned a SPID to your ISDN line. Not all ISDN lines have SPIDs.	`1600(config)#`	**isdn spid2** *555987602*
Step 5	Enable IPX routing on this interface.	`1600(config-if)#`	**ipx network** *123*
Step 6	Disable IPX fast switching on this interface.	`1600(config-if)#`	**no ipx route-cache**
Step 7	Set the router to respond to a local server watchdog packets on behalf of a remote client (called *spoofing*).	`1600(config-if)#`	**ipx watchdog-spoof**
Step 8	Configure this interface to place a call to multiple sites and to authenticate calls from multiple sites based on IPX address and dialer string (phone number). The value *123* represents the IPX network number of the ISDN network. The value *0000.0c03.ecc6* represents the IPX address of the central-site router. The name you enter after the **name** keyword in this command must match the name entered with the **username** command in the previous "Configuring Security" section.	`1600(config-if)#`	**dialer map ipx** *123.0000.0003.eccb* **name** *HQ* **broadcast** *5552053*
Step 9	Assign the dialer interface to a dialer group.	`1600(config-if)#`	**dialer-group** *1*

		Prompt	Command
Step 10	Disable weighted fair queueing for this interface.	`1600(config-if)#`	**`no fair-queue`**
Step 11	Set the encapsulation method on this interface to PPP.	`1600(config-if)#`	**`encapsulation ppp`**
Step 12	Enable CHAP and PAP authentication on this interface. CHAP authentication is attempted first. If the central-site router does not support CHAP, PAP is used for authentication.	`1600(config-if)#`	**`ppp authentication chap pap callin`**
Step 13	Enable multilink PPP on this interface.	`1600(config-if)#`	**`ppp multilink`**
Step 14	Enable the interface and the configuration changes you have just made on the interface.	`1600(config-if)#`	`no shutdown`
Step 15	Exit configuration mode for the BRI interface.	`1600(config-if)#`	`exit`

Verifying Your Configuration

You can verify your configuration to this point by

- Confirming the ISDN Line Status.
- Confirming the IPX Route on the Ethernet Interface.
- Confirming Multilink PPP Configuration.

Confirming the ISDN Line Status

Step 1 From the privileged EXEC command mode, enter the **show isdn status** command.

Step 2 You should see command output similar to the following:

```
1600# show isdn status
The current ISDN Switchtype = basic-5ess
ISDN BRI0 interface
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 80, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        No Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 0
    Total Allocated ISDN CCBs =
```

Step 3 Confirm that the current ISDN switch type (shown in bold in the example) matches the actual switch type that you are using.

Step 4 Confirm that the "Layer 1 status: ACTIVE" message (shown in bold in the example) appears in the command output.

Step 5 Confirm that the "State = MULTIPLE_FRAME_ESTABLISHED" message (shown in bold in the example) appears in the command output.

Note In some cases, you might see a "State = TEI_ASSIGNED" message instead of the "State = MULTIPLE_FRAME_ESTABLISHED" message. This message also means that the ISDN line is correctly configured.

Step 6 To continue configuration, re-enter global configuration mode.

Tips

If you are still having problems, do the following:

- Make sure that you entered the **no shutdown** command while in interface configuration mode for the ISDN interface. This enables the configuration changes that you made on the interface.
- Make sure that any external NT-1 is functioning correctly. Refer to the documentation that came with the NT-1.
- Make sure the ISDN line is correctly configured by checking with the ISDN service provider.

Confirming the IPX Route on the Ethernet Interface

Step 1 From the privileged EXEC command mode, enter the **show ipx route** command:

```
1600# show ipx route 123
Codes: C - Connected primary network,    c - Connected secondary
network
       S - Static, F - Floating static, L - Local (internal), W -
IPXWAN
       R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
       s - seconds, u - uses

2 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

C        123 (PPP),           BR0
```

Step 2 Confirm that the IPX network number (shown in bold in the example) matches the IPX network number that you configured with the **ipx network** command when you configured the Ethernet interface.

Step 3 To continue configuration, re-enter global configuration mode.

Confirming Multilink PPP Configuration

Step 1 From the privileged EXEC command mode, enter the **show ppp multilink** command.

Step 2 Confirm that the "Master link is Virtual-Access1" message (shown in bold in the example) appears in the command output

```
1600# show ppp multilink

Bundle HQ, 1 member, Master link is Virtual-Access1
Dialer Interface is BRI0
  0 lost fragments, 0 reordered, 0 unassigned, sequence 0x0/0x0
rcvd/sent
 0 discarded, 0 lost received, 1/255 load

Member Link: 1
BRI0:1
```

Step 3 To continue configuration, re-enter global configuration mode.

Configuring When the Router Dials Out

Use this table to configure some parameters that control how and when the router dials the central-site router, including:

- Access lists, so that specific types of data trigger a call to the remote site and control the amount of time that your router remains connected to the remote site when no specific type of data is being sent.
- A dialer list, which controls the how and when the router dials the remote site, based on the access lists.

		Prompt	Command
Step 1	Define a standard access list based on IPX network variables.	1600(config)#	**access-list** *900 deny any any all any 457*
Step 2	Define a standard access list based on IPX network variables.	1600(config)#	**access-list** *900 deny rip any rip any rip*

Step 3	Define a standard access list based on IPX network variables.	1600(config)#	**access-list** *900 deny sap any sap any sap*
Step 4	Define a standard access list based on IPX network variables.	1600(config)#	**access-list** *900 permit any any all any all*
Step 5	Specify an access list by list number and protocol (IPX) to define the "interesting" packets that can trigger a called to the destination.	1600(config)#	**dialer-list** *1* **protocol ipx list** *900*

Verifying Your Configuration

You can verify your configuration to this point by

- Confirming Connectivity to the Central-Site Router.
- Confirming the ISDN Interface Configuration.

Confirming Connectivity to the Central-Site Router

Step 1 From the privileged EXEC command mode, enter the **ping** command. The output should be similar to the following:

```
1600# ping ipx 123.0000.0c03.ecc6

Type escape sequence to abort.
Sending 5, 100-byte IPX cisco Echoes to 123.0000.0c03.ecc6, timeout is
2 seconds:
.
*Mar  1 03:52:35.134: %LINK-3-UPDOWN: Interface BRI0:1, changed state
to up
*Mar  1 03:52:35.531: %LINEPROTO-5-UPDOWN: Line protocol on Interface
BRI0:1, changed state to up!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 44/44/44 ms
1600#
*Mar  1 03:52:35.539: %LINK-3-UPDOWN: Interface Virtual-Access1,
changed state to up
*Mar  1 03:52:36.531: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to up
*Mar  1 03:52:38.542: %ISDN-6-CONNECT: Interface BRI0:1 is now
connected to 5552053 HQ
```

Step 2 Verify the following in the command output:

- The address shown in the "Target IPX address" line. It should match the address entered in the **dialer map ipx** command.
- Percentage shown in the "Success rate..." line—A success rate of 60 percent (3/5) or greater means that your router is successfully transferring data to the central-site router.

Step 3 To continue configuration, re-enter global configuration mode.

Confirming the ISDN Interface Configuration

Step 1 From the privileged EXEC command mode, enter the **ping** command:

```
1600# ping ipx 123.0000.0c03.ecc6
```

Step 2 Enter the **show interface** command:

```
1600# show interface virtual-access 1

Virtual-Access1 is up, line protocol is up
  Hardware is Virtual Access interface
  MTU 1500 bytes, BW 64 Kbit, DLY 100000 usec, rely 255/255, load
1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  DTR is pulsed for 5 seconds on reset
  LCP Open, multilink Open
Open: IPXCP
Last input 00:00:01, output never, output hang never
  Last clearing of "show interface" counters 00:54:41
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     708 packets input, 150742 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     709 packets output, 157653 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

Step 3 Confirm that the "Open: IPXCP" message (shown in bold in the example) appears in the command output.

Step 4 To continue configuration, re-enter global configuration mode.

Configuring Command Line Access to the Router

Use this table to configure some parameters that control access to the router, including the type of terminal line used with the router, how long the router waits for a user entry before it times out, and the password used to start a terminal session with the router.

		Prompt	Command
Step 1	Specify the console terminal line.	1600(config)#	**line console** *0*
Step 2	Set the interval that the EXEC command interpreter waits until user input is detected.	1600(config-line)#	**exec-timeout** *5*
Step 3	Specify a virtual terminal for remote console access	1600(config-line)#	**line vty** *0 4*
Step 4	Specify a password on the line.	1600(config-line)#	**password** *lineaccess*
Step 5	Enable password checking at terminal session login.	1600(config-line)#	**login**
Step 6	Exit configuration mode.	1600(config-line)#	**end**

Troubleshooting IPX Problems

If you are having problems or the output that you received during the verification steps is very different from what is shown, you can troubleshoot your router with the Cisco IOS **debug** commands. The **debug** commands provide extensive command output that is not included in this document.

Caution If you are not familiar with Cisco IOS debug commands, you should read the "Using Debug Commands" section in the "Cisco IOS Basic Skills" chapter before attempting any debugging.

Following are **debug** commands that are helpful when troubleshooting ISDN with IPX routing. Follow these commands with the **ping** command to begin debug output:

```
debug dialer events
debug isdn q931
debug ppp negotiation
debug ppp authentication
debug ppp multilink events
```

ISDN Leased Line

This section describes how to configure the router so that it uses the ISDN line as a leased line connection to the central-site router. In the previous configurations in this chapter, the ISDN line functions as a switched connection to the central-site router. It only dials the central-site router when it detects specified types and amounts of data traffic. In a leased line configuration, the ISDN line is always active and connected to the central office switch.

In addition to the assumptions described in the "Before You Begin" section at the beginning of this chapter, this configuration is based on the additional assumption that both ISDN B channels are connecting to the same central-site router.

This configuration describes how to configure the router for IP and IPX. If you followed the configuration instructions for IP and IPX in the previous sections of this chapter, you might not have to do all of the steps shown in this section.

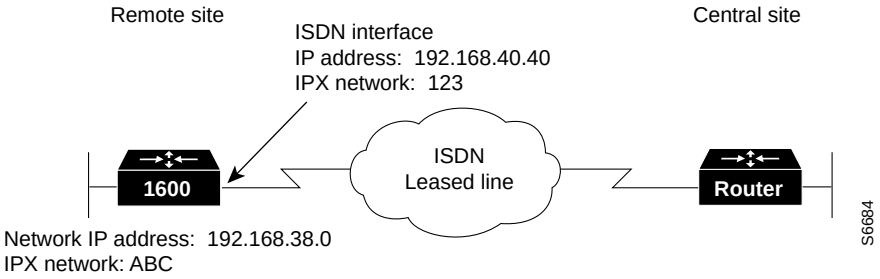
These are major tasks when configuring your router:

- Configuring Global Parameters
- Configuring Security
- Configuring IPX Routing
- Configuring the ISDN Line for Leased Line
- Configuring the ISDN Interface

- Configuring the ISDN Subinterfaces
- Configuring Command Line Access to the Router

Figure 3-3 illustrates the example configuration that is used in this section.

Figure 3-3 ISDN Leased Line Example Configuration



Configuring Global Parameters

Use this table to configure the router for some global parameters, including the ISDN switch type that the router is connected to through the ISDN line, and how log and debug messages are timestamped.

		Prompt	Command
Step 1	Enter configuration mode.	Router#	configure terminal
Step 2	Configure the router to show the date and time of all debug messages. This command is optional, but recommended if you use debug commands to troubleshoot your configuration.	Router(config)#	service timestamps debug datetime msec

		Prompt	Command
Step 3	Configure the router to show the date and time of all log messages. This command is optional, but recommended if you use the verification steps described in this guide. This feature is enabled for all the example command output shown in this guide.	Router(config)#	service timestamps log datetime msec
Step 4	Configure the type of central office switch being used on the ISDN interface. Use the keyword that matches the ISDN switch type that you are using: • **basic-ts013** —Australian TS013 switches • **basic-1tr6** —German 1TR6 ISDN switches • **basic-nwnet3**—Norway NET3 switches (phase 1) • **basic-net3**—NET3 ISDN switches • **vn2**—French VN2 ISDN switches • **vn3**—French VN3 ISDN switches • **ntt**—Japanese NTT ISDN switches • **basic-5ess**—AT&T basic rate switches • **basic-dms100**—NT DMS-100 basic rate switches • **basic-ni1**—National ISDN-1 switches • **basic-nznet3**—New Zealand Net3 switches	Router(config)#	**isdn switch-type** *basic-ni1*

Configuring Security

Use this table to configure the router with some security measures, including the password used to access the router and the username and password used for Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) authentication with the central-site router.

		Prompt	Command
Step 1	Specify a password to prevent unauthorized access to the router.	`Router(config)#`	**enable password** *1600user*
Step 2	Configure the router with a host name, which is used in prompts and default configuration file names. For PPP authentication, the host name entered with this command must match the username of the central-site router.	`Router(config)#`	**hostname** *1600*
Step 3	Specify the password used during caller identification and CHAP and PAP authentication. For CHAP and PAP authentication, the username entered with this command must match the host name of the central-site router.	`1600(config)#`	**username** *HQ* **password** *guessme*

Configuring IPX Routing

Use this command to enable IPX routing on the router. The default setting for the router is IPX routing disabled.

```
1600(config)#ipx routing xxxx.xxxx.xxxx
```

Configuring the ISDN Line for Leased Line

Use this table to set up the ISDN line for a leased line configuration.

		Prompt	Command
Step 1	Define a virtual template from which this multilink PPP bundle interface can replicate its interface parameters.	1600(config)#	**multilink virtual-template** *1*
Step 2	Configure the BRI interface to use the ISDN physical connection as a leased-line service.	1600(config)#	**isdn leased-line BRI0**

Configuring the Ethernet Interface

Use this table to configure the Ethernet interface with IP and IPX network addresses and for multilink PPP.

		Prompt	Command
Step 1	Enter configuration mode for the Ethernet interface.	`1600(config)#`	**interface Ethernet0**
Step 2	Configure this interface with an IP address and a subnet mask.	`1600(config-if)#`	**ip address** *192.168.38.42 255.255.255.0*
Step 3	Configure this interface with an IPX network address.	`1600(config-if)#`	**ipx network** *ABC*
Step 4	Associate the virtual template with this virtual template interface.	`1600(config-if)#`	**interface Virtual-Template***1*
Step 5	Configure the virtual template interface with an IP address and a subnet mask.	`1600(config-if)#`	**ip address** *192.168.40.40 255.255.255.0*
Step 6	Configure the virtual template interface with an IPX network address.	`1600(config-if)#`	**ipx network** *123*
Step 7	Set the encapsulation method on this interface to PPP.	`1600(config-if)#`	**encapsulation ppp**
Step 8	Enable multilink PPP on this interface.	`1600(config-if)#`	**ppp multilink**
Step 9	Enable the interface and the configuration changes you have just made on the interface.	`1600(config-if)#`	`no shutdown`
Step 10	Exit configuration mode for this interface.	`1600(config-if)#`	`exit`

Configuring the ISDN Interface

Use this table to clear the IP address from the ISDN interface. In the following section, you configure two ISDN subinterfaces, which are used for sending data to the central site.

		Prompt	Command
Step 1	Enter configuration mode for the BRI interface.	`1600(config)#`	**`interface BRI0`**
Step 2	Disable IP routing on the BRI0 interface.	`1600(config-if)#`	**`no ip address`**
Step 3	Exit configuration mode for this interface.	`1600(config-if)#`	`exit`

Configuring the ISDN Subinterfaces

Use this table to create and configure two ISDN subinterfaces, including the following:

- PPP packet encapsulation, so that the router can use specific PPP functions.
- Multilink PPP, so that the router can send data to the same destination over multiple point-to-point data links.

		Prompt	Command
Step 1	Enter configuration mode for the BRI0:1 subinterface	`1600(config-if)#`	**`interface BRI0:1`**
Step 2	Enable IP routing on this interface without assigning an IP address.	`1600(config-if)#`	**`ip unnumbered Virtual-Template`***`1`*
Step 3	Set the encapsulation method on this interface to PPP.	`1600(config-if)#`	**`encapsulation ppp`**
Step 4	Enable multilink PPP on this interface.	`1600(config-if)#`	**`ppp multilink`**
Step 5	Enter configuration mode for the BRI0:2 subinterface	`1600(config-if)#`	**`interface BRI0:2`**
Step 6	Enable IP routing on this interface without assigning an IP address.	`1600(config-if)#`	**`ip unnumbered Virtual-Template`***`1`*

		Prompt	Command
Step 7	Set the encapsulation method on this interface to PPP.	`1600(config-if)#`	**`encapsulation ppp`**
Step 8	Enable multilink PPP on this interface.	`1600(config-if)#`	**`ppp multilink`**
Step 9	Exit configuration mode for this interface.	`1600(config-if)`	`exit`

Configuring Dynamic IP Routing

Use this table to configure the router for dynamic IP routing.

		Prompt	Command
Step 1	Configure the router to forward packets addressed to a subnet of a network with no network default route.	`1600(config)#`	**`ip classless`**
Step 2	Specify dynamic routing.	`1600(config)#`	**`ip route 0.0.0.0 0.0.0.0`** *`192.168.40.41`*

Verifying Your Configuration

You can verify your configuration by confirming connectivity to the central-site router.

Step 1 From the privileged EXEC command mode, enter the **ping** command followed by the IP address of the central-site router:

```
1600# ping 192.168.37.40

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.37.40, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 40/43/48 ms
1600#
*Mar  1 03:37:46.526: %LINK-3-UPDOWN: Interface BRI0:1, changed state
to up
*Mar  1 03:37:46.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
BRI0:1, changed state to up
```

```
*Mar  1 03:37:46.939: %LINK-3-UPDOWN: Interface Virtual-Access1,
changed state to up
*Mar  1 03:37:47.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to up
 *Mar  1 03:35:57.217: %ISDN-6-CONNECT: Interface BRI0:1 is now
connected to 5552053 HQ
```

Step 2 Note the percentage in the "Success rate..." line (shown in bold in the example). A success rate of 60 percent (3/5) or greater means that your router is successfully transferring data to the central-site router.

Step 3 If the router is not successfully transferring data to the central-site router (if the success rate is less than 60 percent), take the following steps:

- Use the **show ip route** command to confirm that the routing table entries for the central-site router are correct.
- Use the **show interface bri0** command to confirm that the ISDN interface is active and that IPCP, IPXCP, and Multilink are shown as "Open."

Step 4 To continue configuration, re-enter global configuration mode.

Configuring Command Line Access to the Router

Use this table to configure some parameters that control access to the router, including the type of terminal line used with the router, how long the router waits for a user entry before it times out, and the password used to start a terminal session with the router.

		Prompt	Command
Step 1	Specify the console terminal line.	`1600(config)#`	**line console** *0*
Step 2	Set the interval that the EXEC command interpreter waits until user input is detected.	`1600(config-line)#`	**exec-timeout** *5*
Step 3	Specify a virtual terminal for remote console access.	`1600(config-line)#`	**line vty** *0 4*
Step 4	Specify a password on the line.	`1600(config-line)#`	**password** *lineaccess*

		Prompt	Command
Step 5	Enable password checking at terminal session login.	`1600(config-line)#`	**login**
Step 6	Exit configuration mode.	`1600(config-line)#`	**end**

Troubleshooting Leased Line Problems

If you are having problems or the output that you received during the verification steps is very different from what is shown, you can troubleshoot your router with the Cisco IOS **debug** commands. The **debug** commands provide extensive command output that is not included in this document.

Caution If you are not familiar with Cisco IOS debug commands, you should read the "Using Debug Commands" section in the "Cisco IOS Basic Skills" chapter before attempting any debugging.

Following is the **debug** command that is helpful when troubleshooting dialer profiles with ISDN. Follow this command with the **ping** command to begin debug output:

```
debug ppp negotiation
```

How ISDN Works

ISDN is a set of digital services that is available through your local telephone company. ISDN digitizes information that is sent over the telephone network so that voice, data, text, graphics, music, video, and other material can be sent over existing telephone wire.

ISDN Components

ISDN components include terminals, terminal adapters (TAs), network termination devices, line-termination equipment, and exchange-termination equipment.

ISDN Terminals

There are two type of ISDN terminals:

- Terminal equipment type 1 (TE1) is designed specifically to work with ISDN. TE1s connect to the ISDN network with 4-wire, twisted-pair cable.
- Terminal equipment type 2 (TE2) is non-ISDN equipment (such as DTE) that predates ISDN standards. TE2s connect to the ISDN network with a terminal adapter.

ISDN Network Termination Devices

There are two types of ISDN terminal devices used to connect your router to the telephone company conventional 2-wire local loop:

- Network termination type 1 (NT-1)—In North America, the NT-1 is provided by the customer. In most other parts of the word, the NT-1 is part of the network provided by the ISDN service provider. Cisco 1600 series routers and WAN interface cards that do not have an integrated NT-1 require an external NT-1 to connect to ISDN services. The Cisco 1604 and ISDN BRI U WAN interface card have an integrated NT-1.
- Network termination type 2 (NT-2)—This more complicated device is usually found in digital private branch exchanges (PBXs).

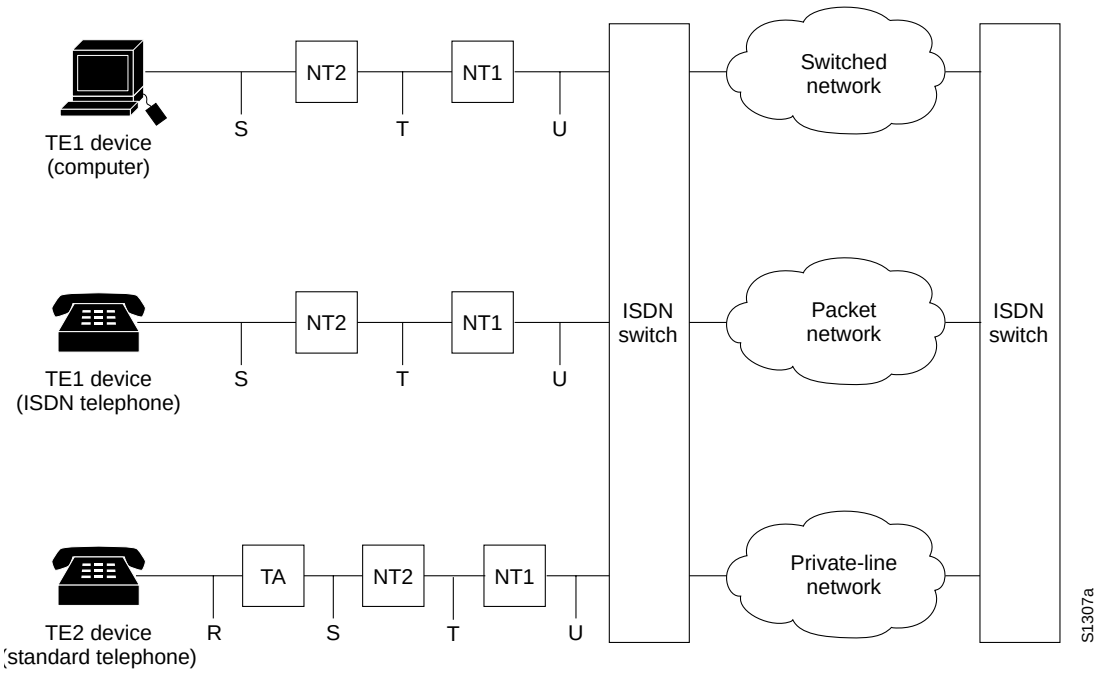
There is also a NT-1/2 device that performs both the functions of an NT-1 and an NT-2.

Sample Configuration

Figure 3-4 shows a sample ISDN configuration with the devices used to connect the user to the ISDN network.

Two of the devices shown, the computer and the ISDN telephone, are compatible with ISDN. The third device, the standard telephone, requires a TA to connect to the ISDN network through an NT-2 or NT-1 device.

Figure 3-4 Sample ISDN Configuration



Services

There are two types of ISDN services:

- Basic Rate Interface (BRI)—This service provides two B channels and one D channel. Each B channel operates at 64 kbps and carries user data. The D channel operates at 16 kbps and carries control and signaling information, although in certain circumstances it carries user data. BRI supports framing control and overhead, and the total bit rate is 192 kbps.
- Primary Rate Interface (PRI)—This service provides 23 B channels (which operate at 64 kbps) and one D channel (which operates at 64 kbps) in North America and Japan, resulting in a bit rate of 1.544 Mbps. In Europe, Australia, and other parts of the world, PRI provides 30 B channels and one D channel.